

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-34164
(P2001-34164A)

(43) 公開日 平成13年2月9日(2001.2.9)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 9 C 1/00	6 2 0	G 0 9 C 1/00	6 2 0 A 5 B 0 1 7
	6 4 0		6 4 0 B 5 J 1 0 4
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 Z
9/10			6 2 1 A
審査請求 有 請求項の数 7 O L (全 19 頁)			

(21) 出願番号 特願平11-209891

(22) 出願日 平成11年7月23日(1999.7.23)

特許法第30条第1項適用申請有り 1999年1月26日～1月29日 電子情報通信学会情報セキュリティ研究専門委員会主催の「1999年暗号と情報セキュリティシンポジウム」において文書をもって発表

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 櫻井 幸一

福岡県福岡市東区箱崎6丁目10番1号 九州大学内

(72) 発明者 宮崎 真悟

東京都府中市東芝町1番地 株式会社東芝府中工場内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

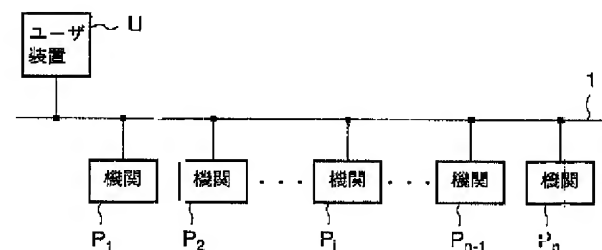
最終頁に続く

(54) 【発明の名称】 秘密分散システム及び記憶媒体

(57) 【要約】

【課題】 本発明は、分配者の無い環境で秘密鍵を算出せずに、 n 個の機関のうち、任意 t 個の機関による分散復号や署名の実現を図る。

【解決手段】 n 個の各機関 $P_1 \sim P_n$ が、 (n, n) 型の1個の部分情報 d_i ($0 \leq i \leq n$)を保持し、部分情報 d_i を (t, n) 型の t ($r+1$)個の部分乱数 S_j とし、 $r+1$ 個の部分乱数 S_j を各機関 P_i の識別番号 z の t 進表示 (t^j 桁目の値 k 、 $0 \leq k \leq t-1$ 、 $0 \leq j \leq r$)に基づいて、各々機関 $P_1 \sim P_n$ に分散し、互いに分散された部分乱数を t 進表示の桁 t^j 毎にまとめて $r+1$ 個の部分情報 $d_{j,k}$ を得る。次に、ユーザ装置 U が t 個の機関 T_z を選択して暗号化データ C を送信し、 t 個の機関 T_z が暗号化データ C を部分情報 $d_{j,k}$ に基づき演算処理して得た部分出力 X_z をそれぞれユーザ装置 U に返信し、ユーザ装置 U が t 個の部分出力 X_z を合成して復号結果を得る秘密分散システム及び記憶媒体。



【特許請求の範囲】

【請求項1】 素因数分解問題に基づく暗号系に用いられ、 n 個の機関に秘密鍵の部分最終情報が分散され、且つ、いずれの機関も自己の部分最終情報だけでは前記秘密鍵を算出不可能な環境にあるとき、前記 n 個の機関のうち、任意の t 個の機関により、前記秘密鍵を算出せずに復号結果及び署名結果を生成可能な (t, n) 型の秘密分散システム。

【請求項2】 公開鍵及び秘密鍵 d を用いるRSA暗号系に適用され、互いにネットワークを介して接続された n 個の機関及びユーザ装置を備え、 n 個の機関に前記秘密鍵 d の部分最終情報が分散されたとき、その中の任意の t 個の機関により、前記秘密鍵 d を算出せずに復号結果又は署名結果を生成可能な (t, n) 型の秘密分散システムであって、

前記 n 個の各機関は、

前記公開鍵及び前記秘密鍵 d を生成する手段と、

この秘密鍵 d に基づいて生成された (n, n) 型の1 個の部分情報 d_i ($0 \leq i \leq n$) を保持する手段と、

t を底とした n の対数 $\log_t n$ 以上の最小の整数を r としたとき、前記部分情報 d_i を (t, n) 型の $t(r+1)$ 個の部分乱数とし、そのうちの $r+1$ 個の部分乱数を前記各機関の識別番号の t 進表示 $(t^j$ 桁目の値 k 、 $0 \leq k \leq t-1$ 、 $0 \leq j \leq r$) に基づいて、それぞれ各機関に分散する手段と、

前記各機関から分散された $n(r+1)$ 個の部分乱数を t 進表示の桁 t^j 毎にまとめて $r+1$ 個の部分最終情報 $d_{j,k}$ を得る手段と、

前記ユーザ装置から受けた処理対象データを前記部分最終情報 $d_{j,k}$ に基づいて演算処理し、得られた部分出力を前記ユーザ装置に返信する手段とを有し、

前記ユーザ装置は、

前記 t 個の機関を選択し、この選択した t 個の各機関に処理対象データを送信する手段と、

前記 t 個の各機関から受信した部分出力を合成して前記復号結果又は署名結果を得る手段とを備えたことを特徴とする秘密分散システム。

【請求項3】 第1の公開鍵 (e, N) 及び秘密鍵 d と、第2の公開鍵 (L^2, N) とを用いるRSA暗号系 $(e$ と L^2 とは最大公約数が1であり、法 N は共通) に適用され、互いにネットワークを介して接続された n 個の機関及びユーザ装置を備え、 n 個の機関に前記秘密鍵 d の部分情報 s_j が分散されたとき、その中の任意の t 個の機関により、前記秘密鍵 d を算出せずに復号結果を生成可能な (t, n) 型の秘密分散システムであって、前記 n 個の各機関は、

前記ユーザ装置から受けた復号対象データ $C_2 (= M^e \pmod{N})$ を演算処理して得られた部分出力 Z_j を前記ユーザ装置に返信する手段とを有し、前記ユーザ装置は、

前記 n 個の機関のうちの t 個の機関を選択し、この選択した t 個の各機関に前記復号対象データ C_2 を送信する手段と、

前記 t 個の各機関から受信した部分出力 Z_j を合成して前記復号結果 $C_1 (= M^{L^2} \pmod{N})$ 、 $^{\wedge}$ はべき乗を示す記号) を得る手段と、

前記復号結果 C_1 、前記処理対象データ C_2 及び下記式に基づいて、演算処理を実行し、最終復号結果 M を求める手段とを備えたことを特徴とする秘密分散システム。

$$a_1 = (L^2)^{-1} \pmod{e}$$

$$a_2 = (a_1 L^2 - 1) / e$$

$$M = C_1^{a_1} (C_2^{a_2})^{-1} \pmod{N}$$

【請求項4】 請求項3に記載の秘密分散システムにおいて、

前記復号対象データ C_2 に代えて、署名対象データ $S_2 (= M)$ を用い、

前記復号結果 C_1 に代えて、署名結果 $S_1 (= M^d L^{\wedge 2} \pmod{N})$ 、 $^{\wedge}$ はべき乗を示す記号) を用い、

前記最終復号結果 M を求める手段に代えて、

前記署名結果 $S_1 (= (M^d)^e)$ 、前記署名対象データ $S_2 (= (M^d)^{L^{\wedge 2}})$ 及び下記式に基づいて、演算処理を実行し、最終署名結果 M^d を求める手段とを備えたことを特徴とする秘密分散システム。

$$a_1 = (L^2)^{-1} \pmod{e}$$

$$a_2 = (a_1 L^2 - 1) / e$$

$$M^d = S_1^{a_1} (S_2^{a_2})^{-1} \pmod{N}$$

【請求項5】 公開鍵及び秘密鍵 d を用いるRSA暗号系に適用され、互いにネットワークを介して接続された n 個の機関及びユーザ装置を備え、 n 個の機関に前記秘密鍵 d の部分最終情報が分散されたとき、その中の任意の t 個の機関により、前記秘密鍵 d を算出せずに復号結果又は署名結果を生成可能な (t, n) 型の秘密分散システムに使用されるコンピュータ読み取り可能な記憶媒体であって、

前記 n 個の各機関内のコンピュータに、

前記公開鍵及び前記秘密鍵 d を生成する手段と、

この秘密鍵 d に基づいて生成された (n, n) 型の1 個の部分情報 d_i ($0 \leq i \leq n$) を保持する手段と、

t を底とした n の対数 $\log_t n$ 以上の最小の整数を r としたとき、前記部分情報 d_i を (t, n) 型の $t(r+1)$ 個の部分乱数とし、そのうちの $r+1$ 個の部分乱数を前記各機関の識別番号の t 進表示 $(t^j$ 桁目の値 k 、 $0 \leq k \leq t-1$ 、 $0 \leq j \leq r$) に基づいて、それぞれ各機関に分散する手段と、

前記各機関から分散された $n(r+1)$ 個の部分乱数を t 進表示の桁 t^j 毎にまとめて $r+1$ 個の部分最終情報 $d_{j,k}$ を得る手段、

前記ユーザ装置から受けた処理対象データを前記部分最終情報 $d_{j,k}$ に基づいて演算処理し、得られた部分出力を前記ユーザ装置に返信する手段、

を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項6】 第1の公開鍵 (e, N) 及び秘密鍵 d と、第2の公開鍵 (L^2, N) とを用いるRSA暗号系 $(e$ と L^2 とは最大公約数が1であり、法 N は共通)に適用され、互いにネットワークを介して接続された n 個の機関及びユーザ装置を備え、 n 個の機関に前記秘密鍵 d の部分情報 s_j が分散されたとき、その中の任意の t 個の機関により、前記秘密鍵 d を算出せずに復号結果を生成可能な (t, n) 型の秘密分散システムに使用される記憶媒体であって、

前記 n 個の各機関内のコンピュータに、

前記ユーザ装置から受けた復号対象データ $C_2 (= M^e \pmod{N})$ を演算処理して得られた部分出力 Z_j を前記ユーザ装置に返信する手段、を実現させるためのプログラムを記憶し、

前記ユーザ装置内のコンピュータに、

前記 n 個の機関のうち t 個の機関を選択し、この選択した t 個の各機関に前記復号対象データ C_2 を送信する手段、

前記 t 個の各機関から受信した部分出力 Z_j を合成して前記復号結果 $C_1 (= M^{L^2} \pmod{N})$ 、 $^{\wedge}$ はべき乗を示す記号)を得る手段、

前記復号結果 C_1 、前記処理対象データ C_2 及び下記式に基づいて、演算処理を実行し、最終復号結果 M を求める手段、

を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

$$a1 = (L^2)^{-1} \pmod{e}$$

$$a2 = (a1L^2 - 1) / e$$

$$M = C_1^{a1} (C_2^{a2})^{-1} \pmod{N}$$

【請求項7】 請求項6に記載の記憶媒体において、前記復号対象データ C_2 に代えて、署名対象データ $S_2 (= M)$ を用い、

前記復号結果 C_1 に代えて、署名結果 $S_1 (= M^d \pmod{N})$ 、 $^{\wedge}$ はべき乗を示す記号)を用い、

前記最終復号結果 M を求める手段に代えて、

前記署名結果 $S_1 (= (M^d)^e)$ 、前記署名対象データ $S_2 (= (M^d)^{L^2})$ 及び下記式に基づいて、演算処理を実行し、最終署名結果 M^d を求める手段とを実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

$$a1 = (L^2)^{-1} \pmod{e}$$

$$a2 = (a1L^2 - 1) / e$$

$$M^d = S_1^{a1} (S_2^{a2})^{-1} \pmod{N}$$

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、素因数分解問題に基づく暗号系の秘密分散システム及び記憶媒体に係り、特に、 n 個の機関に秘密鍵を秘密分散し、その中の任意

の t 個の機関により、秘密鍵を算出せずに分散復号及び署名を実現し得る秘密分散システム及び記憶媒体に関する。

【0002】

【従来の技術】従来、素因数分解問題に基づく暗号系として、例えばRSA暗号系を用いた秘密分散の分野では、しきい値法と呼ばれる秘密分散方式がある。ここで、しきい値法は、秘密情報を n 個の部分情報に分散したとき、 n 個中の t 個の部分情報により秘密情報を完全に復元するが、 $t-1$ 個の部分情報では秘密情報を全く復元できないという、しきい値 t を境にした秘密情報の復元特性をもっている(なお、 $1 < t < n$)。

【0003】この種の秘密分散方式としては、RSA暗号系に、しきい値法の概念を導入し、秘密鍵を (t, n) 型で秘密分散させる (t, n) 型の秘密分散方式が知られている(Y. Frankel, P. Gemmell, P. D. MacKenzie and M. Yung, Optimal-resilience proactive public-key cryptosystems, 38th Annual Symposium on Foundations of Computer Science, pp. 384-393, 1997.

(以下、文献[FGMY97]という)、及びT. Okamoto, Threshold key-recovery systems for RSA, Security Protocols, LNCS 1361, pp. 191-200, 1997. (以下、文献[Ok97]という))。

【0004】中でも、文献[FGMY97]は、ディーラー(分配者)の存在する環境において、秘密鍵 d を算出せずに、任意 t 個の機関で復号や署名の可能な方式を示している。すなわち、合成数 N の異なる素因数を知るディーラーが、素因数を知らなくても任意の t 個の部分情報で復号や署名の可能な秘密鍵 d を作成可能な方式である。

【0005】一方、ディーラーの存在しない環境において、しきい値法ではなく、全ての機関で鍵生成を行う

(n, n) 型の秘密分散方式が知られている(D. Boneh and M. Franklin, Efficient generation of shared RSA keys, Advances in Cryptology-CRYPTO 97, LNCS 1294, pp. 425-439, 1997. (以下、文献[BF97]という))。

【0006】文献[BF97]の方式では、鍵生成を実行すると、秘密鍵 d に対して (n, n) 型の秘密分散が同時に行われる。また、保持する部分情報を用いた全ての機関からの部分出力を合成することにより、秘密鍵 d を算出せずに暗号文を復号可能となっている。

【0007】詳しくは、文献[BF97]では、以下にアルゴリズムを示すように、 $(2, 2)$ 型の秘密分散から $(2, n)$ 型の秘密分散($n \geq 3$ を効率的に構築する方式が述べられている。

【0008】なお、説明の簡単のため、秘密鍵 d を知るユーザがいて、このユーザが秘密鍵 d を $(2, n)$ 型で秘密分散すると仮定する。また、機関 P の総数 n に対し、部分情報の組合せを示す秘密分散多項式の個数は、

$r+1$ であるとし、 $r = \lceil \log n \rceil$ であるとする
(本明細書中、「 $\lceil \cdot \rceil$ 」は、その括弧内の値以上の最小の整数を示す)。

【0009】まず、ユーザは、 $(2, 2)$ 型の秘密分散を $r+1$ 回実行するため、 $r+1$ 個の独立多項式 $d = d_{0,0} + d_{0,1} = d_{1,0} + d_{1,1} = \dots = d_{r,0} + d_{r,1}$ を個別に作成する。

【0010】次に、総数 n の機関における個々の機関の識別番号を z とし($z \in [0, n]$)、識別番号 z の2進表示を $z(2) = \beta_r \beta_{r-1} \dots \beta_0$ とする。ユーザは、0番目 $\sim n$ 番目の全ての機関 $P_0 \sim P_n$ を対象とし、順次、 z 番目の機関 P_z に、 $r+1$ 個の部分情報： $\{d_{r,\beta_r}, d_{r-1,\beta_{r-1}}, \dots, d_{0,\beta_0}\}$ を送る。これにより、全ての機関 $P_0 \sim P_n$ には、識別番号 z の2進表示に対応する部分情報の集合が配送される。

【0011】配送完了後、機関の番号を唯一に設定することで、任意の2個の機関 P_i, P_j ($i \neq j$)は、 $r+1$ 個の $(2, 2)$ 型の部分情報のうち、番号 $z(2)$ で互いにビット β の異なる同一桁 i の部分情報($d_{i,0}, d_{i,1}$)から、秘密鍵 d を復元可能となっている($d_{i,0} + d_{i,1} = d$)。

【0012】次に、上述した $(2, 2)$ 型から $(2, n)$ 型の秘密分散を構築する方式のように、秘密分散の型を拡張するための関連技術について述べる。この種の技術としては、 $(t, 1)$ 型を用いた $(t, 1^m)$ 型の秘密分散方式がある(S. R. Blackburn, M. Burmester, Y. Desmedt and P. R. Wild, Efficient multiplicative sharing schemes, Advances in Cryptology-EUROCRYPT 96, pp. 107-118, 1996. (以下、文献[BBDW96]という))。但し、文献[BBDW96]の方式は、正の整数 m に対し、次の(1)式を満たす 1 に関するものである。

【0013】

【数1】

$$t \geq \binom{t}{2}(m-1) \quad \dots(1)$$

ここで、 $b = \binom{t}{2}(m-1)$ となると、

【0014】

$$t=2 \quad b \geq 1 \rightarrow 1 \geq 1$$

$$t=3 \quad b \geq 3 \rightarrow 1 \geq 3$$

$$t=4 \quad b \geq 6 \rightarrow 1 \geq 6$$

となり、 $t \geq 4$ では $t < 1$ となる。すなわち、 $t \geq 4$ では、 (t, t) 型を用いた (t, n) 型の秘密分散方式を構築不可能となっている。

【0015】このため、以下では、同文献[BBDW96]における $(3, 3)$ 型を用いた $(3, 3^3)$ 型の秘密分散方式を説明する。 $m=2, 1=3, t=3$ とし、(2)式に示すように、 b を算出する。

【0016】

【数2】

$$b = \binom{t}{2}(m-1) = 3 \quad \dots(2)$$

【0017】まず、 $(3, 3)$ 型の秘密分散を $b+1=4$ 回実行し、(3)式に示すように、秘密鍵 d に対する4つの独立多項式を構築する。

【0018】

$$\begin{aligned} d &= d_{0,0} + d_{0,1} + d_{0,2} & (1 \text{ 回目}) \\ &= d_{1,0} + d_{1,1} + d_{1,2} & (2 \text{ 回目}) \\ &= d_{2,0} + d_{2,1} + d_{2,2} & (3 \text{ 回目}) \\ &= d_{3,0} + d_{3,1} + d_{3,2} & (4 \text{ 回目}) \quad \dots(3) \end{aligned}$$

また、 $f(x) = a_0 + a_1 X \pmod{3}$ とする。

【0019】ここで、同文献[BBDW96]では、最終的な機関(ここでは 3^2 個の機関)の集合を P^* としたとき、 $f(X)$ は(4)式のように記載される(pp.113の1行目、なお、式中の“ d ”は、本明細書中では“ m ”と表記した)。

【0020】

【数3】

$$f(X) = \sum_{i=0}^{d-1} a_i X^{i \in P^*} \quad \dots(4)$$

【0021】しかしながら、この(4)式は、次の(5)式の誤りと推測される。

【0022】

【数4】

$$f(X) = \sum_{i=0}^{d-1} a_i X^{i \pmod{\ell}} \quad \dots(5)$$

【0023】但し、 $a_0, a_1 \in F_3$ であり、 $f(\infty) = a_1$ とする。

【0024】

$$f_1(x) = 0 \pmod{3}$$

$$f_2(x) = 1 \pmod{3}$$

$$f_3(x) = 2 \pmod{3}$$

$$f_4(x) = 0 + X \pmod{3}$$

$$f_5(x) = 1 + X \pmod{3}$$

$$f_6(x) = 2 + X \pmod{3}$$

$$f_7(x) = 0 + 2X \pmod{3}$$

$$f_8(x) = 1 + 2X \pmod{3}$$

$$f_9(x) = 2 + 2X \pmod{3}$$

各機関 f_j は($d_{0,f_j(\infty)}, d_{1,f_j(0)}, d_{2,f_j(1)}, d_{3,f_j(2)}$)を持つ。具体的に各機関に保管される部分情報の集合は図12に示す通りであり、機関の組合せと対象の部分情報は図13に示す通りである。

【0025】図12に示すように、例えば機関 f_1, f_4, f_8 (2行目)で分散復号を行う際は、 $X = \infty$ に対応する部分情報を取り出す。それぞれ($d_{0,0}, d_{0,1}, d_{0,2}$)による計算を行い、秘密鍵 d に相当する出力を算出可能となっている。

【0026】また、図13中、a~1のいずれかのアルファベット符号の付された組合せは、各機関の同一の組合せにおいて、秘密鍵dに相当する出力の算出ルートが3種類あることを示している（なお、図13中の“d”は単なるアルファベット符号であり、秘密鍵dではない）。例えば符号bの付された機関の組合せ（f1, f2, f3）では、X=0, 1, 2の何れでも秘密鍵dを回復する3個の部分情報を揃えることが可能である。

【0027】また一方、上述した文献[B F 97]における（n, n）型の秘密分散方式に対し、しきい値法の概念を導入した方式がある（Y. Frankel, P. D. MacKenzie and M. Yung, Robust efficient distributed RSA-key generation, Proceedings of the thirtieth annual ACM symposium on theory of computing, pp. 663-672, 1998.（以下、文献[FMY98]という））。

【0028】文献[FMY98]の方式では、文献[B F 97]の（n, n）型の秘密分散に基づく（t, n）型の鍵生成・共有方式が示されている。具体的には、まず（n, n）型の鍵生成を行い、秘密鍵dに対する和の多項式を生成する。次に、各機関P_iは、部分情報d_iのディーラーとなり、Sum-to-Poly（和から複数個へ）の変換を行う。このとき、各機関P_iは、全ての機関P_jからの部分情報d_jに対する共有情報を合成し、最終的に秘密鍵dに対する秘密分散を行って、秘密鍵dの（t, n）型の秘密共有を実現する。

【0029】これにより、文献[FMY98]の方式では、総数n個のうち、任意のt個の機関PがRSA秘密鍵dを算出でき、鍵回復が可能となっている。

【0030】

【発明が解決しようとする課題】しかしながら以上のような秘密分散システムでは、以下のようにそれぞれ問題がある。文献[BBDW96]の方式では、t=3におけるn>3²の場合とt≥4の場合には（t, 1ⁿ）型の秘密分散の構築が不可であるため、（2, n）型の秘密分散の構築手法が一般化されていない。

【0031】また一方、文献[FMY98]の方式では、秘密鍵dを算出せずに、秘密鍵dを用いた署名や復号を試みる時には問題を生じる。例えば、公開鍵（e, N）で暗号化された暗号文C=M^e（mod N）があるとする。この暗号文Cを任意のt個の機関（この集合をΛとする）で復号するとき、各機関P_jは、（6）式のようなラグランジュの補間係数λ_{j,Λ}を算出し、この補間係数λ_{j,Λ}からそれぞれ部分出力を得る必要がある。

【0032】

【数5】

$$\lambda_{j,\Lambda} = \prod_{\ell \in \Lambda \setminus \{j\}} \frac{\ell}{\ell - j} \pmod{\phi(N)} \quad \dots(6)$$

【0033】しかしながら、いずれの機関P_jも合成数N（=p q）の素因数を知らないため、巾の位数φ

（N）を法とした1-jの乗法逆元が算出不可能となり、ラグランジュの補間係数λ_{j,Λ}も算出不可能となる。よって、ラグランジュの補間係数λ_{j,Λ}を算出時に使う部分出力が算出不可能となり、（7）式の如き、部分出力の合成により平文を復元するための分散復号が実行不可能になってしまう。

【0034】

【数6】

$$\prod_{j \in \Lambda} C^{s_j \lambda_{j,\Lambda}} = C^d = M \pmod{N} \quad \dots(7)$$

【0035】本発明は上記実情を考慮してなされたもので、分配者の無い環境で秘密鍵を算出せずに、n個の機関のうち、任意t個の機関による分散復号や署名を実現し得る（t, n）型の秘密分散システム及び記憶媒体を提供することを目的とする。

【0036】

【課題を解決するための手段】請求項1に対応する発明は、素因数分解問題に基づく暗号系に用いられ、n個の機関に秘密鍵の部分最終情報が分散され、且つ、いずれの機関も自己の部分最終情報だけでは前記秘密鍵を算出不可能な環境にあるとき、前記n個の機関のうち、任意のt個の機関により、前記秘密鍵を算出せずに復号結果及び署名結果を生成可能な（t, n）型の秘密分散システムである。

【0037】また、請求項2に対応する発明は、公開鍵及び秘密鍵dを用いるRSA暗号系に適用され、互いにネットワークを介して接続されたn個の機関及びユーザ装置を備え、n個の機関に前記秘密鍵dの部分最終情報が分散されたとき、その中の任意のt個の機関により、前記秘密鍵dを算出せずに復号結果又は署名結果を生成可能な（t, n）型の秘密分散システムであって、前記n個の各機関としては、前記公開鍵及び前記秘密鍵dを生成する手段と、この秘密鍵dに基づいて生成された

（n, n）型の1個の部分情報d_i（0≤i≤n）を保持する手段と、tを底としたnの対数log_t n以上の最小の整数をrとしたとき、前記部分情報d_iを（t, n）型のt（r+1）個の部分乱数とし、そのうちのr+1個の部分乱数を前記各機関の識別番号のt進表示（t^j桁目の値k、0≤k≤t-1、0≤j≤r）に基づいて、それぞれ各機関に分散する手段と、前記各機関から分散されたn（r+1）個の部分乱数をt進表示の桁t^j毎にまとめてr+1個の部分最終情報d_{j,k}を得る手段と、前記ユーザ装置から受けた処理対象データを前記部分最終情報d_{j,k}に基づいて演算処理し、得られた部分出力を前記ユーザ装置に返信する手段とを有し、前記ユーザ装置としては、前記t個の機関を選択し、この選択したt個の各機関に処理対象データを送信する手段と、前記t個の各機関から受信した部分出力を合成して前記復号結果又は署名結果を得る手段とを備えた秘密分散システムである。

【0038】また、請求項3に対応する発明は、第1の公開鍵 (e, N) 及び秘密鍵 d と、第2の公開鍵 (L^2, N) とを用いるRSA暗号系 $(e$ と L^2 とは最大公約数が1であり、法 N は共通)に適用され、互いにネットワークを介して接続された n 個の機関及びユーザ装置を備え、 n 個の機関に前記秘密鍵 d の部分情報 s_j が分散されたとき、その中の任意の t 個の機関により、前記秘密鍵 d を算出せずに復号結果を生成可能な (t, n) 型の秘密分散システムであって、前記 n 個の各機関としては、前記ユーザ装置から受けた復号対象データ $C2$ ($=M^e \pmod{N}$)を演算処理して得られた部分出力 Z_j を前記ユーザ装置に返信する手段とを有し、前記ユーザ装置としては、前記 n 個の機関のうちの t 個の機関を選択し、この選択した t 個の各機関に前記復号対象データ $C2$ を送信する手段と、前記 t 個の各機関から受信した部分出力 Z_j を合成して前記復号結果 $C1$ ($=M^{L^2} \pmod{N}$)、 $^{\wedge}$ はべき乗を示す記号)を得る手段と、前記復号結果 $C1$ 、前記処理対象データ $C2$ 及び下記式に基づいて、演算処理を実行し、最終復号結果 M を求める手段とを備えた秘密分散システムである。

【0039】

$$a1 = (L^2)^{-1} \pmod{e}$$

$$a2 = (a1L^2 - 1) / e$$

$$M = C_1^{a1} (C_2^{a2})^{-1} \pmod{N}$$

さらに、請求項4に対応する発明は、請求項3に対応する秘密分散システムにおいて、前記復号対象データ $C2$ に代えて、署名対象データ $S2$ ($=M$)を用い、前記復号結果 $C1$ に代えて、署名結果 $S1$ ($=M^d L^2 \pmod{N}$)、 $^{\wedge}$ はべき乗を示す記号)を用い、前記最終復号結果 M を求める手段に代えて、前記署名結果 $S1$ ($=M^d L^2$)及び下記式に基づいて、演算処理を実行し、最終署名結果 M^d を求める手段とを備えた秘密分散システムである。

【0040】

$$a1 = (L^2)^{-1} \pmod{e}$$

$$a2 = (a1L^2 - 1) / e$$

$$M^d = S_1^{a1} (S_2^{a2})^{-1} \pmod{N}$$

また、請求項5に対応する発明は、公開鍵及び秘密鍵 d を用いるRSA暗号系に適用され、互いにネットワークを介して接続された n 個の機関及びユーザ装置を備え、 n 個の機関に前記秘密鍵 d の部分最終情報が分散されたとき、その中の任意の t 個の機関により、前記秘密鍵 d を算出せずに復号結果又は署名結果を生成可能な (t, n) 型の秘密分散システムに使用されるコンピュータ読み取り可能な記憶媒体であって、前記 n 個の各機関内のコンピュータに、前記公開鍵及び前記秘密鍵 d を生成する手段と、この秘密鍵 d に基づいて生成された (n, n) 型の1個の部分情報 d_i ($0 \leq i \leq n$)を保持する手段と、 t を底とした n の対数 $\log_t n$ 以上の最小の

整数を r としたとき、前記部分情報 d_i を (t, n) 型の $t(r+1)$ 個の部分乱数とし、そのうちの $r+1$ 個の部分乱数を前記各機関の識別番号の t 進表示 $(t^j$ 桁目の値 k 、 $0 \leq k \leq t-1$ 、 $0 \leq j \leq r)$ に基づいて、それぞれ各機関に分散する手段と、前記各機関から分散された $n(r+1)$ 個の部分乱数を t 進表示の桁 t^j 毎にまとめて $r+1$ 個の部分最終情報 $d_{j,k}$ を得る手段、前記ユーザ装置から受けた処理対象データを前記部分最終情報 $d_{j,k}$ に基づいて演算処理し、得られた部分出力を前記ユーザ装置に返信する手段、を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【0041】さらに、請求項6に対応する発明は、第1の公開鍵 (e, N) 及び秘密鍵 d と、第2の公開鍵 (L^2, N) とを用いるRSA暗号系 $(e$ と L^2 とは最大公約数が1であり、法 N は共通)に適用され、互いにネットワークを介して接続された n 個の機関及びユーザ装置を備え、 n 個の機関に前記秘密鍵 d の部分情報 s_j が分散されたとき、その中の任意の t 個の機関により、前記秘密鍵 d を算出せずに復号結果を生成可能な (t, n) 型の秘密分散システムに使用される記憶媒体であって、前記 n 個の各機関内のコンピュータに、前記ユーザ装置から受けた復号対象データ $C2$ ($=M^e \pmod{N}$)を演算処理して得られた部分出力 Z_j を前記ユーザ装置に返信する手段、を実現させるためのプログラムを記憶し、前記ユーザ装置内のコンピュータに、前記 n 個の機関のうちの t 個の機関を選択し、この選択した t 個の各機関に前記復号対象データ $C2$ を送信する手段、前記 t 個の各機関から受信した部分出力 Z_j を合成して前記復号結果 $C1$ ($=M^{L^2} \pmod{N}$)、 $^{\wedge}$ はべき乗を示す記号)を得る手段、前記復号結果 $C1$ 、前記処理対象データ $C2$ 及び下記式に基づいて、演算処理を実行し、最終復号結果 M を求める手段、を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【0042】

$$a1 = (L^2)^{-1} \pmod{e}$$

$$a2 = (a1L^2 - 1) / e$$

$$M = C_1^{a1} (C_2^{a2})^{-1} \pmod{N}$$

また、請求項7に対応する発明は、請求項6に対応する記憶媒体において、前記復号対象データ $C2$ に代えて、署名対象データ $S2$ ($=M$)を用い、前記復号結果 $C1$ に代えて、署名結果 $S1$ ($=M^d L^2 \pmod{N}$)、 $^{\wedge}$ はべき乗を示す記号)を用い、前記最終復号結果 M を求める手段に代えて、前記署名結果 $S1$ ($=M^d L^2$)及び下記式に基づいて、演算処理を実行し、最終署名結果 M^d を求める手段とを実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【0043】

$$a1 = (L^2)^{-1} \pmod{e}$$

$$a2 = (a1L^2 - 1) / e$$

$$M^d = S_1^{a1} (S_2^{a2})^{-1} \pmod{N}$$

(作用) 従って、請求項1, 2, 5に対応する発明は以上のような手段を講じたことにより、n個の各機関が、公開鍵及び秘密鍵dを生成し、この秘密鍵dに基づいて生成された(n, n)型の1個の部分情報 d_i ($0 \leq i \leq n$)を保持し、tを底としたnの対数 $\log_t n$ 以上の最小の整数をrとしたとき、この部分情報 d_i を(t, n)型のt(r+1)個の部分乱数とし、そのうちのr+1個の部分乱数を各機関の識別番号のt進表示(t^j 桁目の値 k , $0 \leq k \leq t-1$, $0 \leq j \leq r$)に基づいて、それぞれ各機関に分散し、各機関から分散されたn(r+1)個の部分乱数をt進表示の桁 t^j 毎にまとめてr+1個の部分最終情報 $d_{j,k}$ を得る。

【0044】続いて、ユーザ装置が、t個の機関を選択し、この選択したt個の各機関に処理対象データを送信し、t個の機関が、ユーザ装置から受けた処理対象データを部分最終情報 $d_{j,k}$ に基づいて演算処理し、得られた部分出力をユーザ装置に返信し、ユーザ装置が、t個の各機関から受信した部分出力を合成して復号結果又は署名結果を得る。

【0045】このように、分配者の無い環境で秘密鍵を算出せずに、n個の機関のうち、任意t個の機関による分散復号や署名を実現することができ、また、ラグランジュ補間法を用いず、高い処理効率を実現することができる。

【0046】また、請求項3, 6に対応する発明は、第1の公開鍵(e, N)及び秘密鍵dと、第2の公開鍵(L^2 , N)とを用いるRSA暗号系(eと L^2 とは最大公約数が1であり、法Nは共通)において、n個の機関に秘密鍵dの部分情報 s_j が分散されたとき、ユーザ装置が、n個の機関のうちのt個の機関を選択し、この選択したt個の各機関に復号対象データC2を送信し、t個の各機関が、ユーザ装置から受けた復号対象データC2($=M^e \pmod{N}$)を演算処理して得られた部分出力 Z_j をユーザ装置に返信し、ユーザ装置が、t個の各機関から受信した部分出力 Z_j を合成して復号結果C1($=M^{L^2} \pmod{N}$)を得ると共に、復号結果C1、処理対象データC2及び所定の式($a1 = (L^2)^{-1} \pmod{e}$ 、 $a2 = (a1L^2 - 1) / e$ 、 $M = C_1^{a1} (C_2^{a2})^{-1} \pmod{N}$)に基づいて、演算処理を実行し、最終復号結果Mを求める。

【0047】これにより、分配者の無い環境で秘密鍵を算出せずに、n個の機関のうち、任意t個の機関による分散復号を実現することができ、また、所定条件の公開鍵を用いたラグランジュ補間法に基づき、高い確実性を実現することができる。

【0048】さらに、請求項4, 7に対応する発明は、前記復号対象データC2に代えて、署名対象データS2

($=M$)を用い、復号結果C1に代えて、署名結果S1($=M^d \pmod{N}$)、 \wedge はべき乗を示す記号)を用い、最終復号結果Mを求める手段に代えて、署名結果S1($=M^e \pmod{N}$)、署名対象データS2($=M^d \pmod{N}$)及び所定の式($a1 = (L^2)^{-1} \pmod{e}$ 、 $a2 = (a1L^2 - 1) / e$ 、 $M^d = S_1^{a1} (S_2^{a2})^{-1} \pmod{N}$)に基づいて、演算処理を実行し、最終署名結果 M^d を求める。

【0049】これにより、請求項3, 6に対応する作用と同様の作用を署名処理において実現することができる。

【0050】

【発明の実施の形態】次に、本発明の各実施形態について図面を参照して説明する。なお、第1の実施形態は、ラグランジュ補間法を用いず、高い処理効率を実現したものであり、第2の実施形態は、所定条件の公開鍵を用いたラグランジュ補間法に基づき、高い確実性を実現したものであって、両者ともノンディーラーモデルのしきい値法による分散復号及び署名の可能な(t, n)型の秘密分散システムとなっている。以下、順次説明する。

【0051】(第1の実施形態)本実施形態は、文献[B F 97]における(2, 2)型から(2, n)型の秘密分散を構築する方式を一般化した(t, n)型の秘密分散システムである。具体的には、文献[B F 97]の方式を用いて各機関 P_i が秘密鍵dの(n, n)型の部分情報 d_i を保持すると、全ての機関 $P_1 \sim P_n$ がそれぞれ部分情報 d_i を(t, n)型の部分乱数情報として分配し、各機関 $P_1 \sim P_n$ が部分乱数情報を桁毎にまとめて複数の部分情報 $d_{j,k}$ を得る(t, n)型の秘密分散システムとなっている。

【0052】図1は本発明の第1の実施形態に係る秘密分散システムの構成を示す模式図である。この秘密分散システムは、各々計算機システムとしてのn個の機関 $P_1 \sim P_n$ 及びユーザ装置Uが互いにネットワークを介して接続されている。

【0053】なお、各機関 $P_1 \sim P_n$ は、互いに同一構成を有するので、ここでは任意の機関 P_i (但し、 $1 \leq i \leq n$)を代表例として説明する。

【0054】機関 P_i は、公開鍵(e, N)及び秘密鍵dを生成する機能と、[B F 97]の方式に基づいて、秘密鍵dを(2, n)型の部分情報とし、そのうちのr+1個の部分情報をそれぞれ各機関 $P_1 \sim P_n$ に分散する機能と、分散されたr+1個の部分情報に基づいて、(n, n)型の1個の部分情報 d_i を保持する機能と、この部分情報 d_i を(t, n)型の部分乱数とし、そのうちのr+1個の部分乱数を機関の識別番号のt進表示に基づいて、それぞれ各機関 $P_1 \sim P_n$ に分散する機能と、各機関 $P_1 \sim P_n$ から分散されたn(r+1)個の部分乱数をt進表示の桁 t^j 毎にまとめてr+1個の部分情報 $d_{j,k}$ を得る機能と、ユーザ装置Uから受けた暗

号文Cを復号処理して得られた部分出力Xzをユーザ装置Uに返信する機能とをもちている。

【0055】また、各機関Piは、任意のt個が選択された場合、図示しないが、“P”に代えて“T”の表記を用いる。例えば“機関Pz”は選択されているとき、“機関Tz”と表記される。

【0056】ユーザ装置Uは、n個の機関P1～Pnのうちのt個の機関Tzを選択する機能と、公開鍵(e, N)で暗号化された暗号文Cをも個の各機関Tzに送信する機能と、各機関Tzから受信した部分出力Xzを合成して平文Mを得る機能とをもちている。

【0057】次に、各機関P1～Pn及びユーザ装置Uの具体的なハードウェア構成について述べる。具体的には、機関Pi及びユーザ装置Uは、ハードウェア的には図2に示すように、CPU11、コントローラ12、メモリ13、通信デバイス14、ディスプレイ15、キーボード16及びプリンタ17が互いにバス18を介して接続された計算機システムである。

【0058】これらの構成のうち、メモリ13は、いわゆる主記憶(RAM等)と二次記憶装置(ハードディスク等)の双方を含むものである。この主記憶上に読み込まれたプログラムと、このプログラムに従うCPU11の制御とにより、機関Piが行うべき機能が実現される。すなわち、各機関P1～Pn及びユーザ装置Uは、ソフトウェア的には、上述したそれぞれの機能を行うように、互いに異なる構成を有するものである。これらハードウェア及びソフトウェアの結合からなるそれぞれの機能の詳細な内容は、以下の動作説明において詳細に述べる。

【0059】但し、各機関P1～Pnは、ユーザ装置Uから受信したデータを演算処理し、結果をユーザ装置Uに返信するためのハードウェアがあればよいので、例えばディスプレイ15、キーボード16及びプリンタ17などを適宜、省略してもよい。同様に、ユーザ装置Uにおいても、例えばプリンタ17を省略してもよい。

【0060】次に、以上のように構成された秘密分散システムの動作を説明する。

((t, n)型の秘密分散)各機関P1～Pnは、公開鍵(e, N)及び秘密鍵dを生成すると、文献[BF9

$$z = \beta_{r,z} t^r + \beta_{r-1,z} t^{r-1} + \dots + \beta_{j,z} t^j + \dots + \beta_{0,z} \quad \dots (10)$$

簡単のため、(10)式を(11)式のように表記する。

$$z(t) = \beta_{r,z} \quad \beta_{r-1,z} \quad \dots \quad \beta_{j,z} \quad \dots \quad \beta_{0,z} \quad \dots (11)$$

但し、t進値 $\beta_{r,z} \in \{0, \dots, t-1\}$

また、各機関Piは、z(t)における各桁 t^j 毎のt進値 β に基づいて、次に示すr+1個の部分乱数情報を含む集合Sを機関Pzに送信する(ST4)。

【0067】

【数8】

7]の方式に基づいて、秘密鍵dを(2, n)型の部分情報とし、そのうちのr+1個の部分情報をそれぞれ各機関P1～Pnに分散する。

【0061】各機関P1～Pnは、[BF97]の方式によるr+1個の部分情報に基づき、合成数Nにおける互いに異なる2つの素因数p, qと、秘密鍵dとを(n, n)型で秘密共有している。

【0062】すなわち、各機関Pi(1 ≤ i ≤ n)は、図3に示すように、次の(8)式を満たす部分情報diをそれぞれ保管している(ST1)。

【0063】 $d = d_1 + d_2 + \dots + d_n \quad \dots (8)$

次に、全ての各機関Piは、自己の部分情報diのディーラーとして機能する。すなわち、全ての各機関Piは、(9)式に示すように、自己の部分情報diを示す(t, n)型の部分乱数情報Sj, l(0 ≤ j ≤ r, 0 ≤ l ≤ t-2)を生成する(ST2)。但し、 $r = \lceil \log_t n \rceil$ である。

【0064】

【数7】

$$S_{j,t-1}^{(i)} = d_i - \sum_{l=0}^{t-2} S_{j,l} \quad \dots (9)$$

【0065】なお、この部分乱数情報Sj, lの生成処理は、全ての各機関Piが、それぞれ次に示す如き、自己の部分情報diを示すr+1個の独立多項式を作成することと等価である。

【0066】

$$\begin{aligned} d_i &= S_{0,0} + S_{0,1} + \dots + S_{0,t-2} + S_{0,t-1} \\ &= S_{1,0} + S_{1,1} + \dots + S_{1,t-2} + S_{1,t-1} \\ &= \dots \\ &= S_{j,0} + S_{j,1} + \dots + S_{j,t-2} + S_{j,t-1} \\ &= \dots \\ &= S_{r,0} + S_{r,1} + \dots + S_{r,t-2} + S_{r,t-1} \end{aligned}$$

次に、全ての各機関Piは、識別番号をzとしたとき、以下のステップST3～ST4に示すように、各機関Pz(1 ≤ z ≤ n)と互いに部分乱数情報Sj, lを分散しあう。すなわち、機関Pzの識別番号zを(10)式に示すように、t進数に変換する(ST3)。

$$(S_{r,\beta_{r,z}}^{(i)}, S_{r-1,\beta_{r-1,z}}^{(i)}, \dots, S_{0,\beta_{0,z}}^{(i)})$$

【0068】各機関Pzは、自己を含む全ての各機関Piから得た集合Sに基づいて、次の(12)式に示すように、各桁j毎の部分乱数情報Sj, lの総和をとって部分情報dj, kを算出する(ST5)。但し、 $k = \{\beta_{r,z}, \beta_{r-1,z}, \dots, \beta_{0,z}\}$, 0 ≤ j ≤ rである。

【0069】

【数9】

$$d_{j,k} = \sum_{i=1}^n S_{j,k}^{(i)} = S_{j,k}^{(1)} + S_{j,k}^{(2)} + \dots + S_{j,k}^{(n)} \quad \dots(12)$$

【0070】各機関Pz は、桁j の数に対応する r+1

$$\begin{aligned} d &= d_{0,0} + d_{0,1} + \dots + d_{0,t-1} \\ &= d_{1,0} + d_{1,1} + \dots + d_{1,t-1} \\ &= \dots \\ &= d_{r,0} + d_{r,1} + \dots + d_{r,t-1} \end{aligned}$$

例えば、(3, 27) 型の秘密分散における機関 z=2 の保管情報は、以下の通りである。

【0072】

$$r = \lceil \log_3 27 \rceil = 3$$

$$20 = 0 \times 3^3 + 2 \times 3^2 + 0 \times 3^1 + 2 \times 3^0$$

$$20(3) = 0202 \quad (3\text{進表示})$$

$$\begin{aligned} d &= d_{3,0} + d_{3,1} + d_{3,2} \quad (3^3 \text{ 桁目}) \\ &= d_{2,0} + d_{2,1} + d_{2,2} \quad (3^2 \text{ 桁目}) \\ &= d_{1,0} + d_{1,1} + d_{1,2} \quad (3^1 \text{ 桁目}) \\ &= d_{0,0} + d_{0,1} + d_{0,2} \quad (3^0 \text{ 桁目}) \end{aligned} \quad (14)$$

(分散復号化) n 個の機関 P1 ~ Pn のうち、任意の t 個の機関 Tz (この集合を Λ とする) は、ユーザ装置 U からの復号依頼により、ユーザ装置 U の公開鍵 (e, N) で暗号化されたデータ $C = M^e \pmod{N}$ を図4のステップ ST11 ~ ST16 に示すように分散復号

$$z(t) = \beta_{t,z} \quad \beta_{t-1,z} \quad \dots \quad \beta_{0,z} \quad \dots(15)$$

続いて、ユーザ装置 U は、t 個の機関 Ta, Tb $\in \Lambda$ (a ≠ b) における t 進表示の各桁 t^j ($0 \leq j \leq r$) 毎に、t 進表示の値 β が全て異なる ($\beta_{j,a} \neq \beta_{j,b}$) という条件を満たす桁 t^j が有るか否かを判定する (ST12)。

【0076】この条件を満たす桁 t^j がないとき、この集合 Λ による分散復号は不可能であるため、集合 Λ 内の機関 Tz を多少入れ換えて (ST13)、ステップ ST11 から再実行する。

【0077】ステップ ST2 で条件を満たす桁 t^j があるとき、ユーザ装置 U は、暗号化データ C を各機関 Tz に送信する (ST14)。

【0078】各機関 Tz は、 t^j 桁に対応する部分情報 $d_{j,k}$ ($k = \beta_{j,z}$) に基づいて、暗号化データ C を復号処理し、得られた部分出力 $Xz (= C^{d_{j,k}} \pmod{N})$ をそれぞれユーザ装置 U に返信する (ST15)。

【0079】ユーザ装置は、t 個の各機関 Tz ($z \in \Lambda$) から受信した t 個の部分出力 Xz ($z \in \Lambda$) を (16) 式のように合成し、平文 M を復元することができる (ST16)。

【0080】

【数10】

個の部分情報 $d_{j,k}$ を保管する (ST6)。なお、部分情報 $d_{j,k}$ は、秘密鍵 d の部分集合である。

【0071】秘密鍵 d と部分秘密鍵 $d_{j,k}$ との関係は、以下の (13) 式に示す通りである。

$$\begin{aligned} &(t^0 \text{ 桁目}) \\ &(t^1 \text{ 桁目}) \\ &(\dots) \\ &(t^r \text{ 桁目}) \quad \dots(13) \end{aligned}$$

よって、機関 P_{z_0} は、次の (14) 式に示す全ての部分情報のうち、識別番号 z の 3 進表示 (0202) に対応する部分情報 ($d_{3,0}$, $d_{2,2}$, $d_{1,0}$, $d_{0,2}$) を保管する。

【0073】

化する。

【0074】すなわち、ユーザ装置 U は、(15) 式に示すように、t 個の機関 Tz の識別番号 z をそれぞれ t 進表示に変換する (ST11)。

【0075】

$$\begin{aligned} \prod_{z \in \Lambda} C^{d_{j,1} d_{j,2} \dots d_{j,t}} \\ &= (M^e)^{d_{j,1} d_{j,2} + \dots + d_{j,t}} \quad \dots(16) \\ &= (M^e)^d \\ &= M \pmod{N} \end{aligned}$$

【0081】また、以上の動作は、暗号化データ C ($= M^e \pmod{N}$) を t 個の各機関 Tz に送ることにより、平文 M を分散復号した場合である。これに限らず、本実施形態は、図5に示すように、暗号化データ C に代えて、署名対象データ M を t 個の各機関 Tz に送信したとき (ST14a)、前述した部分出力 Xz の合成により、署名 $M^d \pmod{N}$ を得ることもできる (ST16a)。上述したように本実施形態によれば、n 個の各機関 P1 ~ Pn が、公開鍵及び秘密鍵 d を生成し、この秘密鍵 d に基づいて生成された (n, n) 型の 1 個の部分情報 d_i ($0 \leq i \leq n$) を保持し、t を底とした n の対数 $\log_t n$ 以上の最小の整数を r としたとき、この部分情報 d_i を (t, n) 型の $t(r+1)$ 個の部分乱数 S_j とし、そのうちの $r+1$ 個の部分乱数 S_j を各機関 Pi の識別番号 z の t 進表示 (t^j 桁目の値 k , $0 \leq k \leq t-1$, $0 \leq j \leq r$) に基づいて、それぞれ各機関 P1 ~ Pn に分散し、これら分散された $n(r+1)$ 個の部分乱数を t 進表示の桁 t^j 毎にまとめて $r+1$ 個の部分情報 $d_{j,k}$ を得る。

【0082】続いて、ユーザ装置Uが、 t 個の機関 T_z を選択して暗号化データC（又は署名対象データ）を送信し、 t 個の機関 T_z が、暗号化データC（又は署名対象データ）を部分情報 $d_{j,k}$ に基づいて演算処理し、得られた部分出力 X_z をそれぞれユーザ装置Uに返信し、ユーザ装置Uが、 t 個の部分出力 X_z を合成して復号結果（又は署名結果）を得る。

【0083】このように、分配者の無い環境で秘密鍵を算出せずに、 n 個の機関のうち、任意 t 個の機関による分散復号や署名を実現することができる。また、復号分散時に、ラグランジュの補間係数を算出する手間を省略でき、高い処理効率を実現することができる。

【0084】また、本実施形態は、予め暗号文への入力を表として保持でき、ラグランジュの補間係数の算出が不要な分だけ、文献[FMY98]の方式よりも、演算の処理効率を向上させることができる。

【0085】さらに、本実施形態は、全ての組合せに応じたラグランジュの補間係数を表として保管する場合、文献[FMY98]の方式よりも、保管する情報の量を低減させることができる。

【0086】例えば、文献[FMY98]の方式は、ラグランジュの補間法に基づくしきい値法を用いた分散復号化を行う。ここでは、秘密鍵 d が各機関 $P_1 \sim P_n$ のもつ部分情報の単純和ではなく、各機関 P_j は、前述したラグランジュの補間係数 $\lambda_{j,\Lambda}$ を算出し、合成する必要がある。よって、補間係数 $\lambda_{j,\Lambda}$ を予め算出して表に

$$C^{d_{1,0}} \cdot C^{d_{1,1}} \cdot C^{d_{1,2}} = M^{e_d} \\ = M \pmod{N} \quad \dots (17)$$

ところが、 P_{23} に代えて P_{11} を用いた各機関 P_{20} 、 P_{23} 、 P_{11} では、復号操作は失敗する。すなわち、各機関の3進表示は、 $P_{20}=0202$ 、 $P_{23}=0212$ 、 $P_{11}=0102$ であり、それぞれの保管情報は図7に示す通りである。

【0090】この場合、秘密鍵 d を構成する3つの部分情報（ $d_{j,0} + d_{j,1} + d_{j,2}$ ）がどの桁 j でも揃わず、いずれかの部分情報が2つ以上の機関において重複（衝突）している。このように保管する部分情報の重複により、分散復号の不可能な場合がある。

【0091】この場合、別の t 個の機関を選択し直す必要がある。ここで、機関の総数 n が大きく、 t 個以上の機関を比較的自由に選択可能な場合、本実施形態の（ t, n ）型の秘密分散が適している。すなわち、機関の総数 n が大きいときには復号不能となっても、 t 個の機関 P を再編成して分散復号プロトコルをし直せばよい。

【0092】逆に n の数が小さく、機関 P の選択の余地がない場合は、全ての組合せに応じた関係式を作成する方式が適している。例えば、エルガマル(ElGamal)暗号系では、 n 個のうちの任意の t 個の機関がグループの鍵で暗号化された暗号文を復号することができる技術が提

保管する場合、1つの部分情報と参加機関 T_z の全ての組合せに応じた $n \cdot C_t$ 個の補間係数 $\lambda_{j,\Lambda}$ を算出して保管する必要がある。

【0087】一方、本実施形態では、「 $\log_t n$ 」+1個の部分情報から機関の組合せに対応する部分情報を選択すればよい。よって、保管される部分情報は、「 $\log_t n$ 」+1個でよく、少ない情報量となっている。

【0088】ところで、本実施形態の方式によれば、 t 個の機関の組合せが悪いとき、暗号文を分散復号できない場合がある。この場合について（3, 27）型の秘密分散を例に挙げて補足的に説明する。今、秘密鍵 d について、以下の $r+1$ 個の多項式が成立しているとする。

$$\begin{aligned} d &= d_{3,0} + d_{3,1} + d_{3,2} \quad (3^3 \text{ 桁目}) \\ &= d_{2,0} + d_{2,1} + d_{2,2} \quad (3^2 \text{ 桁目}) \\ &= d_{1,0} + d_{1,1} + d_{1,2} \quad (3^1 \text{ 桁目}) \\ &= d_{0,0} + d_{0,1} + d_{0,2} \quad (3^0 \text{ 桁目}) \end{aligned}$$

まず、分散復号が可能な場合を示す。27個の機関のうち、機関 P_{20} 、 P_{23} 、 P_{26} が分散復号プロトコルに介入するとき、復号操作 $C^d = M^{e_d} = M$ は成功する。ここで、各機関 P_{20} 、 P_{23} 、 P_{26} の3進表示は、 $P_{20}=0202$ 、 $P_{23}=0212$ 、 $P_{26}=0222$ であり、それぞれの保管情報は図6に示す通りとなっている。ここで、 3^1 桁に注目すると、（17）式に示すように、 $d = d_{1,0} + d_{1,1} + d_{1,2}$ から d による復号化処理が可能となる。

案されている（T. P. Pedersen, A threshold cryptosystem without a trusted party, Advances in Cryptology-Eurocrypt 91, LNCS 547, pp.522-526, 1991.（以下、文献[Ped91b]という））。すなわち、文献[Ped91b]の方式のように任意の t 個の機関で分散復号・鍵復元を行うには、秘密鍵 d に関する $n \cdot C_t$ 個の独立な関係式を作成すればよい。具体的には、ある組合せ（ Λ ）のときは（18）式のように該当する関係式により分散復号を行う方式である。

【0093】
$$d = d_{1,\Lambda} + d_{2,\Lambda} + \dots + d_{t,\Lambda} \quad \dots (18)$$
しかしながら、文献[Ped91b]の方式では、衝突の可能性はないものの、機関の総数 n に比例して関係式の数が増大になってしまう。よって、衝突の可能性の低い範囲で、独立多項式を最小限に抑えることが好ましい。

【0094】各方式はそれぞれ長所・短所があるので、第1実施形態の方式（再編成する方式）、第1実施形態の方式において関係式を用いる方式、あるいは後述する第2の実施形態の方式（補間法を用いる方式）のいずれを選択するかは、機関の総数 n や処理効率、使用される環境、復号処理不能が許されるか否かなどの条件に応じ

て使い分けることが好ましい。

【0095】(第2の実施形態)次に、本発明の第2の実施形態について説明するが、その前に本実施形態の前提となるRSA共通法誤用プロトコルについて述べる。

【0096】RSA暗号系において、1つのメッセージMを、互いに共通する法Nと、互いに異なる公開指数 e_1 , e_2 とを用いる条件の下でそれぞれ暗号化し、得られた2つの異なる暗号文 C_1 , C_2 があるとすると、この場合、合成数Nの素因数が不明でも、2つの暗号文 C_1 , C_2 からメッセージMを復元できる(G. J. Simmons, A weak privacy protocol using the RSA cryptological algorithm, Cryptologia, vol.7, pp.180-182, 1983. (以下、文献[Sim83]という))。

【0097】この文献[Sim83]の方式において、前述した2つの暗号文 C_1 , C_2 は、次の(19)式～(20)式に示すように得られている。

【0098】

$$C_1 = M^{e_1} \pmod{N} \quad \dots (19)$$

$$C_2 = M^{e_2} \pmod{N} \quad \dots (20)$$

ここで、異なる公開指数 e_1, e_2 の最大公約数 $\gcd(e_1, e_2) = 1$ である場合、以下のステップSTc1～STc3を行うと、2つの暗号文 C_1 , C_2 からメッセージMを復元できる(D. R. Stinson, CRYPTOGRAPHY: Theory and Practice, CRC Press, Inc. Boca Raton, Florida, U. S. A., 1995. (以下、文献[Sti95]という))。

【0099】

(ステップSTc1) $a_1 = e_1^{-1} \pmod{e_2}$

(ステップSTc2) $a_2 = (a_1 e_1 - 1) / e_2$

(ステップSTc3) $M = C_1^{a_1} (C_2^{a_2})^{-1} \pmod{N}$

また、上記処理(Step c1～c3)を次のように表記する。

【0100】Common(e_1, e_2) \rightarrow M

以上のように、RSA暗号系においては、所定の条件を満たすとき、メッセージMを復元可能なプロトコルが存在する。このプロトコルがRSA共通法誤用プロトコルと呼ばれている。

【0101】さて次に、本発明の第2の実施形態に係る秘密分散システムについて説明する。本実施形態は、文献[Sim83]及び[Sti95]等のRSA共通法誤用プロトコルを適用可能な条件で公開鍵を作成し、文献[FMY98]の手法により、秘密鍵dの部分情報 s_j を分散する(t, n)型の秘密分散システムである。

【0102】なお、RSA共通法誤用プロトコルを適用可能な条件とは、次の(a)～(c)を全て満たすことに相当する。

(a) メッセージMが同じである。

(b) 法Nが共通する。

(c) 互いに異なる公開指数(e_1, e_2)の最大公約数 $\gcd(e_1, e_2) = 1$ である。但し、以下の説明では、公開

指数(e_1, e_2)を(L^2, e)と表記している。また、公開指数 L^2 の元となるLは、 $L = n!$ に代えて、 $L = (n-1)!$ としてもよい。また、ユーザ装置及び各機関は、ハードウェア的な構成に関しては図1及び図2に示した通りとし、機能に関しては第1実施形態とは異なるので、以下に説明する。

【0103】なお、各機関 $P_1 \sim P_n$ は、前述同様に、任意の機関 P_i (但し、 $1 \leq i \leq n$)を代表例として説明する。機関 P_i は、[FMY98]の方式に基づいて、法Nの部分情報(p_j, q_j)を作成する機能と、これら部分情報 p_j, q_j をそれぞれ各機関 $P_1 \sim P_n$ に分散する機能と、各機関 P_j の(p_j, q_j)を基に、公開鍵(e, N)を生成する機能と、秘密鍵dから(t, n)型の部分情報 s_j を得る機能と、夫々部分情報(p_j, q_j)及び s_j を保持する機能と、ユーザから受けた暗号文 $C (= C_2 = M^e \pmod{N})$ を復号処理して得られた部分出力 Z_j をユーザ装置Uに返信する機能とをもっている。

【0104】ユーザ装置Uは、 n 個の機関のうちの t 個の機関 T_z を選択する機能と、公開鍵(e, N)で暗号化された暗号文 $C_2 (= M^e \pmod{N})$ を t 個の各機関 T_z に送信する機能と、各機関 T_z から受信した部分出力 Z_j を合成して暗号文 $C_1 (= M^{L^2} \pmod{N})$ を得る機能と、2つの暗号文(M^{L^2}, M^e)から、前述したRSA共通法誤用プロトコルCommon(L^2, e) \rightarrow Mを用いて、メッセージMを算出する機能とをもっている。

【0105】次に、以上のように構成された秘密分散システムの動作を説明する。

((t, n) 型の秘密分散)各機関は互いに、文献[FMY98]の方式に基づいて、秘密鍵dを(t, n)型の部分情報とし、対応する部分情報 s_j を個別に n 個の機関 $P_1 \sim P_n$ に分散する。

【0106】具体的には、各機関 P_j は、法Nの構成要素(p_j, q_j)を作成し、夫々送信する。各機関 P_j は、他の各機関 P_j から受けた(p_j, q_j)の合成 $N = (p_1 + p_2 + \dots + p_n)(q_1 + q_2 + \dots + q_n)$ が異なる2つの素数の積であるか否かを判定し、異なる素数の積であるとき、正当として次に進む。

【0107】各機関 P_j は(p_j, q_j)を基に、公開鍵(e, N)を生成し、各機関 P_j の保持すべき秘密鍵dの部分情報 d_j を算出する((n, n) 型秘密分散完了)。

【0108】 $d = d_1 + d_2 + \dots + d_j + \dots + d_n$
次に、各機関 P_j は、(n, n)型の秘密鍵dをSum-to-Polyの技術により、(t, n)型の秘密鍵dに変換する((t, n) 型秘密分散完了)。

【0109】このとき、 $t-1$ 個の乱数 $\{b_1, \dots, b_{t-1}\}$ Z に対し、(21)式の如き、多項式を定める。

$$f(x) = d + b_1x + b_2x^2 + \dots + b_{t-1}x^{t-1} \quad \dots (21)$$

この式は、 y 切片を秘密鍵 d とした $k-1$ 次の多項式であり、ラグランジュの補間法により、 k 個の座標点 $(j, f(j))$ から一意に定まる性質をもっている。但し、 $k-1$ 個の座標点からは一意に定まらず、任意の y 切片が可能となり、秘密鍵 d を得られない性質もある。

【0110】各機関 P_j は、各機関 $P_1 \sim P_n$ の自己の識別番号 j ($1 \leq j \leq n$)を独立変数 x として上記多項式 $f(x)$ に代入して $f(j)$ を計算し、 $f(x)$ 上の y 座標を示す部分情報 $s_j (= f(j))$ を各機関 P_j 毎に得る。

【0111】各機関 P_j は、得られた (t, n) 型の部分情報 s_j と、予め保持する、法 N の素因数 p, q の部分情報 (p_j, q_j) とを保管する。なお、 (n, n) 型の部分情報 d_j も保持されるが、本実施形態では特に使用されない。

【0112】(分散復号化) n 個の機関のうち、任意の t 個の機関 T_z (この集合を Λ とする)は、ユーザ装置 U からの復号依頼により、ユーザ装置 U の公開鍵 (e, N) で暗号化されたデータ $C = M^e \pmod{N}$ を図8のステップST21～ST24に示すように分散復号化する。ここで、 $L = n!$ かつ最大公約数 $\gcd(e, L$

$^2) = 1$ とする。

【0113】すなわち、ユーザ装置 U は、暗号文 $C (= M^e \pmod{N})$ を t 個の各機関 T_j (Λ)に送信する(ST21)。各機関 T_j は、次の(22)式～(24)式の通り、それぞれ自己の部分情報 s_j を用いて部分出力 Z_j を算出し、得られた部分出力 Z_j をユーザ装置 U に返信する(ST22)。

【0114】

【数11】

$$\lambda_{j,\Lambda} = \prod_{\ell \in \Lambda \setminus \{j\}} \frac{\ell}{\ell - j} \quad \dots (22)$$

$$\sigma_j = s_j \cdot L^2 \cdot \lambda_{j,\Lambda} \quad \dots (23)$$

$$Z_j = C^{\sigma_j \pmod{N}} \quad \dots (24)$$

【0115】ユーザ装置 U は、次の(25)式のように、 t 個の各機関 T_j から受ける部分出力 Z_j を合成し、暗号文 $M^{L^2} \pmod{N}$ を算出する(ST23)。

【0116】

【数12】

$$\prod_{j \in \Lambda} Z_j = (M^e)^{L^2 \sum_{j \in \Lambda} (s_j \lambda_{j,\Lambda})} = M^{L^2 \pmod{N}} \quad \dots (25)$$

【0117】ユーザ装置 U は、元の暗号文 M^e と、この暗号文 M^{L^2} との互いに異なる2つの暗号文 (M^{L^2}, M^e) から、前述したRSA共通法誤用プロトコルCommon $(L^2, e) \rightarrow M$ を用いて、メッセージ M を算出する(ST24)。なお、本実施形態と、前述したプロトコ

$$C_1^{a_1} (C_2^{a_2})^{-1} = M^{L^2 a_1 - e a_2} = M \pmod{N} \quad \dots (26)$$

(分散署名)なお、ユーザ装置 U は、分散復号に限らず、 t 個の機関 T_z に分散署名を行わせてもよい。この場合、ユーザ装置 U は、図9に示すように、復号対象の暗号文 C に代えて、署名対象データ $S_1 (= M)$ を用いて(ST21a)、復号結果の暗号文 M^{L^2} に代えて、署名結果 $S_2 (= (M^d)^{L^2} \pmod{N})$ 、 \wedge はべき乗を示す記号)を用いる(ST23a)。

【0119】そして、ユーザ装置 U は、 $(C_1, C_2) = (M^d \wedge^{L^2}, M) = ((M^d)^{L^2}, (M^d)^e)$ から、

$$C_1^{a_1} (C_2^{a_2})^{-1} = M^{d(L^2 a_1 - e a_2)} = M^d \pmod{N} \quad \dots (27)$$

(分散署名の変形例)なお、上述した分散署名は、図10に示すように変形してもよい。すなわち、ステップST23aの後、ユーザ装置 U は、この署名対象データ S_1 及び署名結果 S_2 の組を図示しない相手先の署名検証装置に送信する(ST25a)。署名検証装置は、署名対象データ S_1 及び第1公開鍵 (e, N) から第1比較データ $D_1 (= M^e \pmod{N})$ を算出し、署名結果 S_2 及び第2公開鍵 (e, N) から第2比較データ

と対応関係は、 $(M^{L^2}, M^e) = (C_1, C_2)$ であり、 $(L^2, e) = (e_1, e_2)$ である。ここで、RSA共通法誤用プロトコルは、(26)式に示すように、健全性を有している。

【0118】

前述同様に、以下のRSA共通法誤用プロトコルに基づいて、署名 M^d を算出する(ST24a)。

【0120】

$$a_1 = (L^2)^{-1} \pmod{e}$$

$$a_2 = (a_1 L^2 - 1) / e$$

$$M = C_1^{a_1} (C_2^{a_2})^{-1} \pmod{N}$$

ここで、RSA共通法誤用プロトコルは、(27)式に示すように、健全性を有している。

【0121】

$D_2 (= M^{L^2} \pmod{N})$ を算出する(ST26a)。

【0122】続いて、署名検証装置は、第1並びに第2比較データ D_1, D_2 及び下記(28)式～(30)式のRSA共通法誤用プロトコルに基づいて、演算処理を実行し、出力 M を求める(ST27a)。

【0123】

$$a1 = (L^2)^{-1} \pmod{e} \quad \dots (28)$$

$$a2 = (a1L^2 - 1) / e \quad \dots (29)$$

$$M = D_1^{a1} (D_2^{a2})^{-1} \pmod{N} \quad \dots (30)$$

ここで、出力Mと署名対象データS1とが一致するとき、署名検証装置は、ユーザ装置Uの署名を正当と認める(ST28a)。上述したように本実施形態によれば、RSA共通法誤用プロトコルを適用可能な条件のRSA暗号系において、n個の機関P1～Pnに秘密鍵dの部分情報sjが分散されたとき、ユーザ装置Uが、t個の機関Tzを選択して暗号化データC1を送信し、t個の各機関Tzが、暗号化データC1(=M^a (mod N))を演算処理して得られた部分出力Zjをユーザ装置に返信し、ユーザ装置Uが、t個の部分出力Zjを合成して復号結果C2(=M^{L²} (mod N))を得ると共に、復号結果C2、処理対象データC1及びRSA共通法誤用プロトコルに基づいて、演算処理を実行し、最終復号結果Mを求める。

【0124】これにより、分配者の無い環境で秘密鍵を算出せずに、n個の機関のうち、任意t個の機関による分散復号を実現することができ、また、所定条件の公開鍵を用いたラグランジュ補間法に基づき、高い確実性を実現することができる。

【0125】さらに、復号対象データC2に代えて、署名対象データS2(=M)を用い、復号結果C1に代え

但し、本実施形態方式は、係数(α, β) = (-a2, a1)であり、

文献[FGMY97]の方式は、係数(α, β) = (P, s/H)である。

【0130】本実施形態方式では、復号時に部分出力Zjを合成した後に、合成出力からユークリッドアルゴリズムによりMを算出するので、このMの算出処理の分だけ、文献[FGMY97]の方式よりも処理効率が低下している(文献[FGMY97]の方式は、ディーラーが鍵分散時にユークリッド公式を作成するので、復号時に各機関の部分出力を合成し、合成出力がメッセージMとなる)。

【0131】しかしながら、文献[FGMY97]の方式は、Nのオイラー関数φ(N)を知るディーラーが必要であり、d = P + L² k (mod φ(N))を満たすL² kを複数の機関に秘密分散して共有する。ここで、ディーラーが秘密鍵dと素因数p, qを紛失した場合、この複数の機関から秘密鍵dを回復できない。理由は、L² kを回復しても、法φ(N)を紛失しているので、L² kから秘密鍵dを算出できないからである。但し、法φ(N)でdに合同なP + L² kを算出することはできる。

【0132】すなわち、文献[FGMY97]の方式では、ディーラーの存在する環境において、分散署名や分散復号を行えるが、ディーラーへのdそのものの鍵回復を行えない。文献[FGMY97]の方式では、鍵回復を行う際に、ディーラーモデルの文献(T. P. Pedersen, Distributed provers with applications to undeni

て、署名結果S1(=M^d L² (mod N)、^はべき乗を示す記号)を用いることにより、RSA共通法誤用プロトコルを用いて、演算処理を実行し、署名M^dを求める。

【0126】これにより、分散復号と同様に、分散署名を行うことができる。すなわち、本実施形態によれば、所定の条件で公開鍵を作成することにより、t個の機関の組合せとは無関係に、確実に復号処理・署名処理を実行することができる。

【0127】なお、ここでノン・ディーラーモデルでの上述した機能を実現する本実施形態方式と、ディーラーモデルでの機能((t, n)型での分散復号/分散署名)を実現する文献[FGMY97]の方式とを比較して述べる。

【0128】本実施形態方式は、文献[FGMY97]の方式と同じく、α, βを係数として次の(30)式のユークリッド公式を前提とする。

$$e^{\alpha} + L^2 \beta = 1 \quad \dots (30)$$

但し、gcd(e, L²) = 1

【数13】

able signatures, Advances in Cryptology-Eurocrypt 91, LNCS 547, pp.221-238, 1991. (以下、文献[Ped91a]という))の方式又は文献[Ok97]の方式といった別の方式を用いる必要がある。ここで、分散RSA暗号系における従来方式及び本発明方式の位置づけを整理すると、各方式は、図11に示すように分類される。

【0133】一方、本発明方式は、ディーラーの存在する環境では、文献[Ped91a]との組合せにより分散署名及び分散復号を実現でき、ディーラーの存在しない環境では、前述した通り、文献[FGMY98]等との組合せにより分散署名及び分散復号を実現することができる。

【0134】なお、上述した第1及び第2の実施形態は、ディーラーの存在しない環境の場合を述べているので、以下に、ディーラーの存在する環境に適用する場合の変形例1, 2について簡単に説明する。

【0135】すなわち、変形例1は、第1の実施形態をディーラーモデルに適用する場合であり、ディーラーとしてのユーザ装置Uは、(13)式を満たす全ての部分秘密鍵dj,kを作成し、各機関に振り分ける作業を行う。この変形例1によれば、前述したステップST1～ST4までの複雑な処理を省略できる分だけ、効率を向上させることができる。

【0136】また、変形例2は、第2の実施形態を文献[Ped91a]と組合せた場合であり、文献[FMY98]と組合せた結果と同じ機能を果たすことができる。

【0137】すなわち、本発明は、 (t, n) 型の秘密分散であれば、ディーラーの有無とは無関係に実現でき、上述した各実施形態に限らず、 n 羽の鳥のうち、任意の t 羽の鳥を異なる巣箱に入れるような関数群(K. Kurosawa and D. Stinson, Personal communication, June 1996 Referred in Desmedts paper. (Y. Desmedt, Some recent research aspects of threshold cryptography, Information Security, LNCS 1396, pp. 158-173, 1997.))を適宜利用して実現することができる。

【0138】尚、本発明における記憶媒体としては、磁気ディスク、フロッピー(登録商標)ディスク、ハードディスク、光ディスク(CD-ROM、CD-R、DVD等)、光磁気ディスク(MO等)、半導体メモリ等、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【0139】また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているOS(オペレーティングシステム)や、データベース管理ソフト、ネットワークソフト等のMW(ミドルウェア)等が本実施形態を実現するための各処理の一部を実行しても良い。

【0140】さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【0141】また、記憶媒体は1つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【0142】尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【0143】また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機

能を実現することが可能な機器、装置を総称している。

【0144】また、本発明は、RSA暗号系に限らず、素因数分解問題に基づく暗号系であれば、RSA暗号系以外の暗号系に適用してもよい。その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【0145】

【発明の効果】以上説明したように本発明によれば、分配者の無い環境で秘密鍵を算出せずに、 n 個の機関のうち、任意 t 個の機関による分散復号や署名を実現できる (t, n) 型の秘密分散システム及び記憶媒体を提供できる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係る秘密分散システムの構成を示す模式図

【図2】同実施形態における各機関及びユーザ装置のハードウェア構成を示すブロック図

【図3】同実施形態における秘密分散動作を説明するためのフローチャート

【図4】同実施形態における復号化動作を説明するためのフローチャート

【図5】同実施形態における署名動作を説明するためのフローチャート

【図6】同実施形態における復号可能な例を説明するための各機関の保管情報を示す模式図

【図7】同実施形態における復号不可能な例を説明するための各機関の保管情報を示す模式図

【図8】本発明の第2の実施形態における復号化動作を説明するためのフローチャート

【図9】同実施形態における署名動作を説明するためのフローチャート

【図10】同実施形態における変形動作を説明するためのフローチャート

【図11】従来方式と本発明方式との位置付けを示す分類図

【図12】従来の方式における各機関に保管される部分情報の集合を示す模式図

【図13】従来の方式における機関の組合せと対象の部分情報を示す模式図

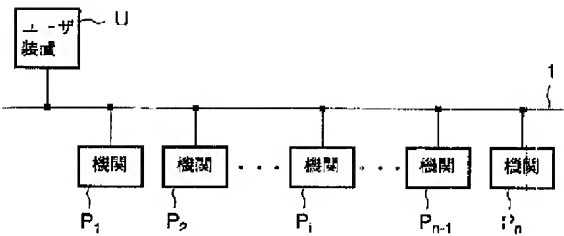
【符号の説明】

1…ネットワーク

U…ユーザ装置

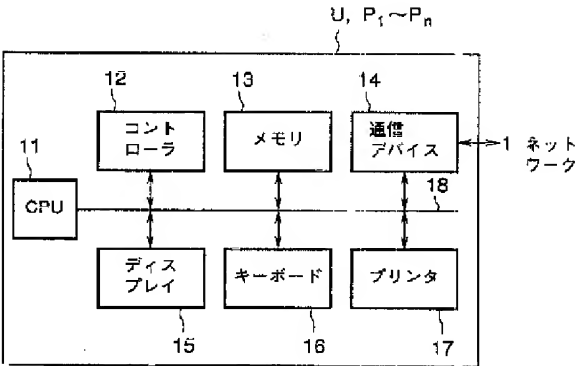
P1 ~ Pn, Pi …機関

【図1】

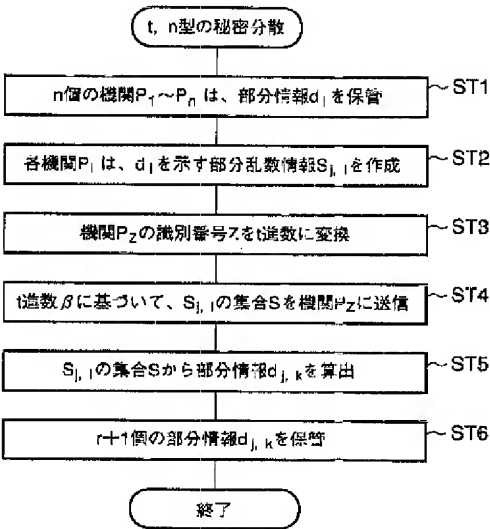


【図3】

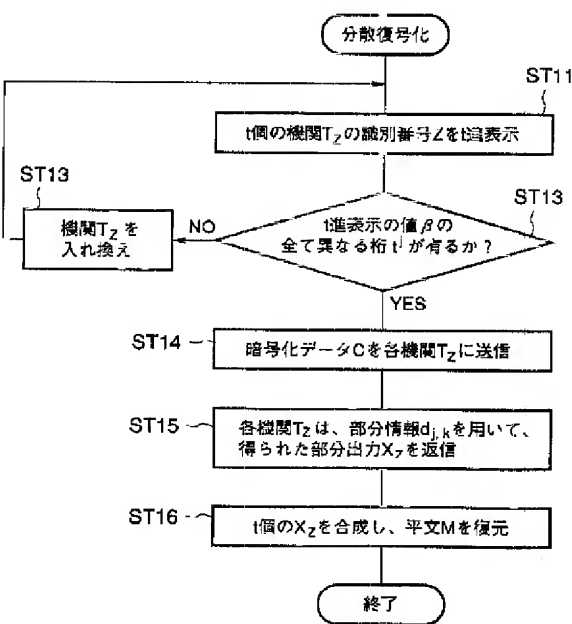
【図2】



【図4】



【図6】

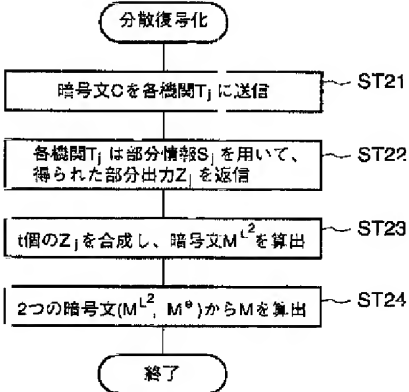


	P ₂₀	P ₂₃	P ₂₆
3 ³ 桁目	d _{3,0}	d _{3,0}	d _{3,0}
3 ² 桁目	d _{2,2}	d _{2,2}	d _{2,2}
3 ¹ 桁目	d _{1,0}	d _{1,1}	d _{1,2}
3 ⁰ 桁目	d _{0,2}	d _{0,2}	d _{0,2}

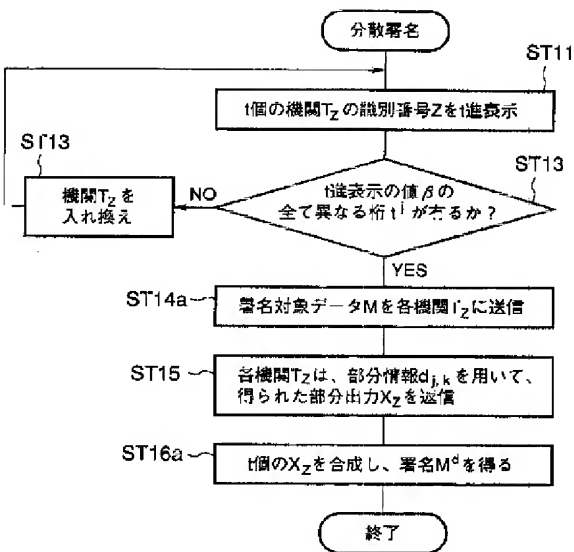
【図7】

	P ₂₀	P ₂₃	P ₁₁
3 ³ 桁目	d _{3,0}	d _{3,0}	d _{3,0}
3 ² 桁目	d _{2,2}	d _{2,2}	d _{2,1}
3 ¹ 桁目	d _{1,0}	d _{1,1}	d _{1,0}
3 ⁰ 桁目	d _{0,2}	d _{0,2}	d _{0,2}

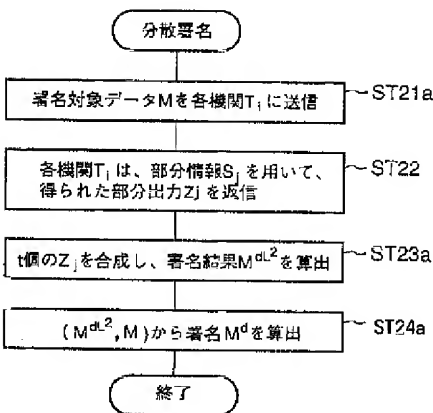
【図8】



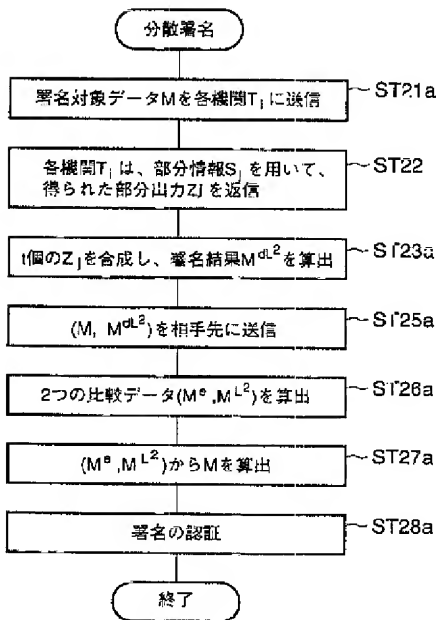
【図5】



【図9】



【図10】



【図11】

	ディーラーあり	ディーラーなし
[t, n] 一鍵回復	<ul style="list-style-type: none">[Ped 91a][Oka 97]	<ul style="list-style-type: none">[FMY 98]
[t, n] 一復号/署名	<ul style="list-style-type: none">[Ped 91a][FGMY 97][Ped 91a] + 本発明 (変形例2)ディーラーモデル + 本発明 (変形例1)	<ul style="list-style-type: none">[BBRW 96][BF 97][FMY 98][BF 97] + 本発明 (第1実施形態)[FMY 98] + 本発明 (第2実施形態)

【図12】

	$X=\infty$	$X=0$	$X=1$	$X=2$
f_1	$d_{0,0}$	$d_{1,0}$	$d_{2,0}$	$d_{3,0}$
f_2	$d_{0,0}$	$d_{1,1}$	$d_{2,1}$	$d_{3,1}$
f_3	$d_{0,0}$	$d_{1,2}$	$d_{2,2}$	$d_{3,2}$
f_4	$d_{0,1}$	$d_{1,0}$	$d_{2,1}$	$d_{3,2}$
f_5	$d_{0,1}$	$d_{1,1}$	$d_{2,2}$	$d_{3,0}$
f_6	$d_{0,1}$	$d_{1,2}$	$d_{2,0}$	$d_{3,1}$
f_7	$d_{0,2}$	$d_{1,0}$	$d_{2,2}$	$d_{3,1}$
f_8	$d_{0,2}$	$d_{1,1}$	$d_{2,0}$	$d_{3,2}$
f_9	$d_{0,2}$	$d_{1,2}$	$d_{2,1}$	$d_{3,0}$

【図13】

	X=∞	X=0	X=1	X=2
a	1, 4, 7	b 1, 2, 3	b 1, 2, 3	b 1, 2, 3
	1, 4, 8	1, 2, 6	1, 2, 5	1, 2, 4
	1, 4, 9	1, 2, 9	1, 2, 7	1, 2, 8
	1, 5, 7	1, 5, 3	1, 4, 3	1, 6, 3
	1, 5, 8	1, 5, 6	1, 4, 5	1, 6, 4
c	1, 5, 9	c 1, 5, 9	a 1, 4, 7	d 1, 6, 8
	1, 6, 7	1, 8, 3	1, 9, 3	1, 7, 3
d	1, 6, 8	d 1, 8, 6	c 1, 9, 5	a 1, 7, 4
	1, 6, 9	1, 8, 9	1, 9, 7	1, 7, 8
	2, 4, 7	4, 2, 3	6, 2, 3	5, 2, 3
	2, 4, 8	4, 2, 6	6, 2, 5	5, 2, 4
e	2, 4, 9	e 4, 2, 9	f 6, 2, 7	g 5, 2, 8
	2, 5, 7	4, 5, 3	6, 4, 3	5, 6, 3
g	2, 5, 8	h 4, 5, 6	h 6, 4, 5	h 5, 6, 4
	2, 5, 9	4, 5, 9	6, 4, 7	5, 6, 8
f	2, 6, 7	i 4, 8, 3	j 6, 9, 3	k 5, 7, 3
	2, 6, 8	4, 8, 6	6, 9, 5	5, 7, 4
	2, 6, 9	4, 8, 9	6, 9, 7	5, 7, 6
	3, 4, 7	7, 2, 3	8, 2, 3	9, 2, 3
l	3, 4, 8	f 7, 2, 6	g 8, 2, 5	e 9, 2, 4
	3, 4, 9	7, 2, 9	8, 2, 7	9, 2, 8
k	3, 5, 7	k 7, 5, 3	i 8, 4, 3	j 9, 6, 3
	3, 5, 8	7, 5, 6	8, 4, 5	9, 6, 4
	3, 5, 9	7, 5, 9	8, 4, 7	9, 6, 8
	3, 8, 7	7, 8, 3	8, 9, 3	9, 7, 3
	3, 6, 8	7, 8, 6	8, 9, 5	9, 7, 4
j	3, 6, 9	i 7, 8, 9	l 8, 9, 7	l 9, 7, 8

【手続補正書】

【提出日】平成12年2月2日(2000. 2. 2)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】0010

【補正方法】変更

【補正内容】

【0010】次に、総数 n の機関における個々の機関の識別番号を z とし($z \in [0, n]$)、識別番号 z の2進表示を $z(2) = \beta_r \beta_{r-1} \dots \beta_0$ とする。ユーザは、0番目 $\sim n$ 番目の全ての機関 $P_0 \sim P_n$ を対象とし、順次、 z 番目の機関 P_z に、 $r+1$ 個の部分情報： $\{d_{r, \beta_r}, d_{r-1, \beta_{r-1}}, \dots, d_{0, \beta_0}\}$ を送る。これにより、全ての機関 $P_0 \sim P_n$ には、識別番号 z の2進表示に対応する部分情報の集合が配送される。

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0023

【補正方法】変更

【補正内容】

【0023】但し、 $a_0, a_1 \in F3$ であり、 $f(\infty) = a_1$ とする。

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0066

【補正方法】変更

【補正内容】

【0066】

$$\begin{aligned}
 di &= S_{0,0} + S_{0,1} + \dots + S_{0,t-2} + S_{0,t-1} \\
 &= S_{1,0} + S_{1,1} + \dots + S_{1,t-2} + S_{1,t-1} \\
 &= \dots \\
 &= S_{j,0} + S_{j,1} + \dots + S_{j,t-2} + S_{j,t-1} \\
 &= \dots \\
 &= S_{r,0} + S_{r,1} + \dots + S_{r,t-2} + S_{r,t-1}
 \end{aligned}$$

次に、全ての各機関 P_i は、識別番号を z としたとき、以下のステップST3 \sim ST4に示すように、各機関 P_z ($1 \leq z \leq n$)と互いに部分乱数情報 $S_{j,1}$ を分散しあう。すなわち、機関 P_z の識別番号 z を(10)式に示すように、 t 進数に変換する(ST3)。

$$z = \beta_{r,z} t^r + \beta_{r-1,z} t^{r-1} + \dots + \beta_{j,z} t^j + \dots + \beta_{0,z} \quad \dots (10)$$

簡単のため、(10)式を(11)式のように表記する。

$$z(t) = \beta_{r,z} \quad \beta_{r-1,z} \quad \dots \quad \beta_{j,z} \quad \dots \quad \beta_{0,z} \quad \dots (11)$$

但し、 t 進値 $\beta_{r,z} \in \{0, \dots, t-1\}$

また、各機関 P_i は、 $z(t)$ における各桁 t^j 毎の t 進値 β に基づいて、次に示す $r+1$ 個の部分乱数情報を含む集合 S を機関 P_z に送信する(ST4)。

【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0068

【補正方法】変更

【補正内容】

【0068】各機関 P_z は、自己を含む全ての各機関 P

$$z(t) = \beta_{r,z} \quad \beta_{r-1,z} \quad \dots \quad \beta_{0,z} \quad \dots (15)$$

続いて、ユーザ装置 U は、 t 個の機関 $T_a, T_b \in \Lambda$ ($a \neq b$)における t 進表示の各桁 t^j ($0 \leq j \leq r$)毎に、 t 進表示の値 β が全て異なる($\beta_{j,a} \neq \beta_{j,b}$)という条件を満たす桁 t^j が有るか否かを判定する(ST12)。

【手続補正6】

【補正対象書類名】明細書

【補正対象項目名】0079

【補正方法】変更

【補正内容】

【0079】ユーザ装置は、 t 個の各機関 T_z ($z \in$

$$f(x) = d + b_1 x + b_2 x^2 + \dots + b_{t-1} x^{t-1} \quad \dots (21)$$

この式は、 y 切片を秘密鍵 d とした $k-1$ 次の多項式であり、ラグランジュの補間法により、 k 個の座標点($j, f(j)$)から一意に定まる性質をもっている。但し、 $k-1$ 個の座標点からは一意に定まらず、任意の y 切片が可能となり、秘密鍵 d を得られない性質もある。

【手続補正8】

【補正対象書類名】明細書

【補正対象項目名】0113

【補正方法】変更

【補正内容】

【0113】すなわち、ユーザ装置 U は、暗号文 $C (= M^e \pmod{N})$ を t 個の各機関 T_j ($j \in \Lambda$)に送信する(ST21)。各機関 T_j は、次の(22)式～(24)式の通り、それぞれ自己の部分情報 s_j を用いて部分出力 Z_j を算出し、得られた部分出力 Z_j をユーザ装置 U に返信する(ST22)。

i から得た集合 S に基づいて、次の(12)式に示すように、各桁 j 毎の部分乱数情報 $S_{j,l}$ の総和をとって部分情報 $d_{j,k}$ を算出する(ST5)。但し、 $k \in \{\beta_{r,z}, \beta_{r-1,z}, \dots, \beta_{0,z}\}$, $0 \leq j \leq r$ である。

【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0075

【補正方法】変更

【補正内容】

【0075】

Λ から受信した t 個の部分出力 X_z ($z \in \Lambda$)を(16)式のように合成し、平文 M を復元することができる(ST16)。

【手続補正7】

【補正対象書類名】明細書

【補正対象項目名】0109

【補正方法】変更

【補正内容】

【0109】このとき、 $t-1$ 個の乱数 $\{b_1, \dots, b_{t-1}\} \in \mathbb{Z}$ に対し、(21)式の如き、多項式を定める。

【手続補正9】

【補正対象書類名】明細書

【補正対象項目名】0131

【補正方法】変更

【補正内容】

【0131】しかしながら、文献[FGMY97]の方式は、 N のオイラー関数 $\phi(N)$ を知るディーラーが必要であり、 $d \equiv P + L^2 k \pmod{\phi(N)}$ を満たす $L^2 k$ を複数の機関に秘密分散して共有する。ここで、ディーラーが秘密鍵 d と素因数 p, q を紛失した場合、この複数の機関から秘密鍵 d を回復できない。理由は、 $L^2 k$ を回復しても、法 $\phi(N)$ を紛失しているため、 $L^2 k$ から秘密鍵 d を算出できないからである。但し、法 $\phi(N)$ で d に合同な $P + L^2 k$ を算出することはできる。

フロントページの続き

F ターム(参考) 5B017 AA06 AA08 BA05 BA07 BA10
BB02 BB07 CA01 CA06 CA07
CA08 CA09 CA11 CA16
5J104 AA01 AA09 AA16 EA02 EA04
EA32 JA27 LA03 LA06 NA02